How to get started analyzing an application threat model

This page has been made public for vendors

Question

How do I get started analyzing an initial application threat model that was provided by the VA Software Assurance Program Office?

Answer

After an initial application threat model is created, it will have been posted in Microsoft Threat Modeling Tool file format (".tm7" file extension) to the same VA network share that was used prior to uploading the design documentation.

Microsoft Threat Modeling Tool software is required in order to view and analyze the application threat model. The VA TRM entry for this software for reference can be found HERE. The following instructions are how to download this software:

1. Go to https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx
2. Select **Related Downloads** then on the **SDL Threat Modeling Tool** link
3. On the download page, optionally select **Details** and **System Requirements** for more information
4. On the download page, click the **Download** button
5. On the download page, select **Install Instructions** then follow provided guidance (administrative permissions are necessary)

The following steps are the basic workflow to analyze the provided threat model file:

1. Open the provided threat model file (with the **.tm7** file extension) using the Microsoft Threat Modeling Tool
2. In either the **Design** or **Analysis** view, select **Reports**, select **Create Full Report**
3. In a web browser, review the **Threat Modeling Report** for each threat
4. In the **Analysis** view:
    a. Review the **Description, Recommendations,** and refer to additional information at https://capec.mitre.org/ about the threat for the **CAPEC-ID**
    b. Update the **Developer Analysis** text field in the **Threat Properties** panel to reflect analysis
    c. Select the appropriate value from the **Status** pull down
5. In the **Design** view, update model elements to adjust or refine as needed
6. Repeat above steps until VA SwA Application Threat Modeling SOP requirements are met
7. Request V&V secure design review validation

VA Secure Design Review SOP requirements are in summary: no model errors, all threats analyzed, and documentation references provided. However, the VA SwA Application Threat Modeling SOP should be consulted for additional details.

Analysis will need to describe how the application is protected against threats such as:

Type of Potential Threat Reported	Example Analysis Required
Spoofing	Check for potential **authentication** issues for the indicated model elements
Tampering	Check for potential **integrity** issues for the indicated model elements
Repudiation	Check for potential **nonrepudiation** issues for the indicated model elements
Information Disclosure	Check for potential **confidentiality** issues for the indicated model elements
Denial of Service	Check for potential **availability** issues for the indicated model elements

Microsoft Threat Modeling Tool Version	2016 and later
Threat Modeling Tool Design View Topic	☐ Yes ☑ No
Threat Modeling Tool Analysis View Topic	☐ Yes ☑ No
Supporting Analysis Documentation Topic	☑ Yes ☐ No
Other Related Topic	☐ Yes ☑ No

Request initial threat models, design review validations, and support HERE.

Elevation of Privilege	Check for potential **authorization** issues for the indicated model elements

References

- Microsoft Threat Modeling Tool
- VA SwA Application Threat Modeling SOP